

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開平8-106382

(43) 公開日 平成 8 年 (1996) 4 月 23 日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0 A	7230-5B		
	K	7230-5B		
G 0 9 C 1/00		7259-5J		
G 1 1 B 19/02	5 0 1 N	7525-5D		

審査請求 未請求 請求項の数15 O L (全 18 頁)

(21) 出願番号 特願平6-225228

(22) 出願日 平成 6 年 (1994) 9 月 20 日

(31) 優先権主張番号 特願平6-219372

(32) 優先日 平 6 (1994) 8 月 10 日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72) 発明者 秋山 良太

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72) 発明者 吉岡 誠

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

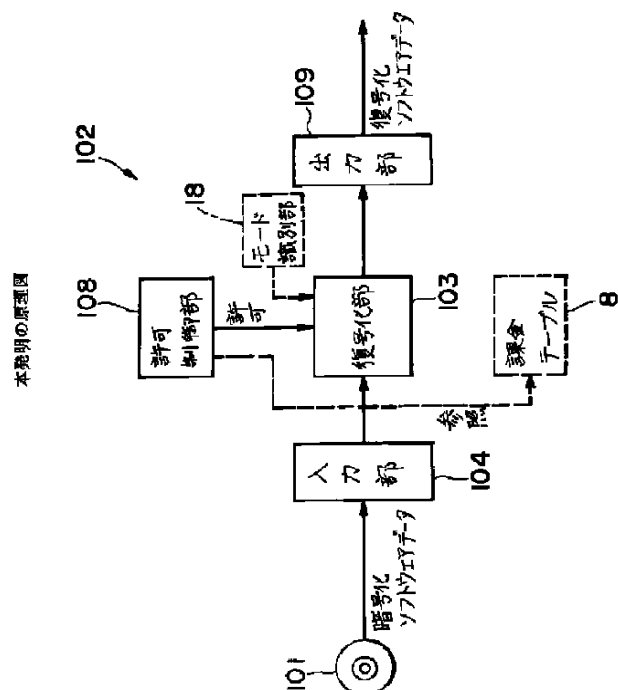
(74) 代理人 弁理士 遠山 勉 (外 1 名)

(54) 【発明の名称】 ソフトウェア管理モジュール、ソフトウェア再生管理装置およびソフトウェア再生管理システム

(57) 【要約】

【目的】 ソフトウェアの格納媒体を複雑にすることなく、より一層のセキュリティチェックと効率的な課金管理の可能なソフトウェアの管理方式を提供する。

【構成】 ソフトウェア格納媒体や通信から得られる暗号化ソフトウェアに対して、ハードウェアに内蔵あるいは着脱可能なソフトウェア管理モジュールを提供し、このソフトウェア管理モジュールには、暗号化されたソフトウェアを復号化する機能を持たせるとともに、許可制御部を設けて復号を許可するか否かを管理するようにした。



【特許請求の範囲】

【請求項1】 暗号化された所定のソフトウェア（プログラムおよび／またはデータ）を選択して再生するためのソフトウェア再生装置に装着されるソフトウェア管理モジュールであって、

前記暗号化ソフトウェアを入力する入力部と、
所定の暗号化ソフトウェアの復号を許可する許可制御部と、

前記許可制御部により許可され前記入力部で入力された暗号化ソフトウェアを復号する復号化部と、

前記復号化部で復号された復号化ソフトウェアを出力する出力部とからなるソフトウェア管理モジュール。

【請求項2】 前記に加えて、課金情報記憶部を備えており、前記許可制御部は当該課金情報記憶部を参照してソフトウェア格納媒体からの所定のソフトウェアの復号を許可する請求項1記載のソフトウェア管理モジュール。

【請求項3】 前記に加えて、暗号化部を備えており、前記許可制御部は暗号化ソフトウェアを復号化して得られたプログラムより発生または加工されたユーザ情報を外部に出力する際に当該暗号化部によって当該ユーザ情報を暗号化する請求項1記載のソフトウェア管理モジュール。

【請求項4】 前記ユーザ情報は課金情報である請求項3記載のソフトウェア管理モジュール。

【請求項5】 前記復号化部は、前記暗号化ソフトウェアの特性に応じて復号化の暗号利用モードを変更可能なモード識別部を備えていることを特徴とする請求項1記載のソフトウェア管理モジュール。

【請求項6】 前記復号化部は、入力側に配置された入力用バッファと、

入力データに対して所定の論理による暗号化または復号化を実行する復号化実行部と、 前記復号化実行部の前段に配置された中間レジスタと、

前記入力レジスタと、前記中間レジスタの間に配置され、前記入力レジスタからの出力と復号化実行部からの出力とのいずれかを選択的に前記中間レジスタに出力するセレクトと、

前記復号化実行部の次段に設けられ復号化されたデータを順次出力する出力用バッファとからなる請求項1記載のソフトウェア管理モジュール。

【請求項7】 前記入力用バッファまたは出力用バッファはシフトレジスタである請求項6記載のソフトウェア管理モジュール。

【請求項8】 暗号化された所定のソフトウェアを格納した格納媒体から暗号化ソフトウェアを読み出すドライブ装置と、

前記格納媒体より暗号化ソフトウェアを読み込んで復調する復調手段と、

前記暗号化ソフトウェアを入力する入力部と、所定の暗

号化ソフトウェアの復号を許可する許可制御部と、前記許可制御部により許可され前記で入力された暗号化ソフトウェアを復号する復号化部と、前記復号化部で復号された復号化ソフトウェアを出力する出力部とからなるソフトウェア管理モジュールと、

前記管理モジュールから出力された復号化ソフトウェアを出力する出力手段とからなるソフトウェア再生装置。

【請求項9】 前記請求項8において、ソフトウェア管理モジュールを内蔵したカード媒体を装着可能なカードドライブ装置を備えている請求項8記載のソフトウェア再生装置。

【請求項10】 管理センタとソフトウェア再生装置とからなり、

前記管理センタは、前記ソフトウェア再生装置からの使用要求に対して鍵情報を許諾コマンドとして発行する許諾コマンド発行手段を有しており、

前記ソフトウェア再生装置は、前記鍵情報に基づいて前記ソフトウェアの復号化を実行する復号手段を備えているソフトウェア再生管理システム。

【請求項11】 前記管理センタは、ユーザの課金情報を蓄積する課金情報蓄積手段を有しており、前記ソフトウェア再生装置が課金情報を前記管理センタに通知する際に当該情報を暗号化する暗号化手段を備えていることを特徴とする請求項10記載のソフトウェア再生管理システム。

【請求項12】 前記管理センタは、暗号化または非暗号化ソフトウェアよりチェックサムを生成する送信側チェックサム生成部を有し、

前記ソフトウェア再生装置は、前記管理センタより前記ソフトウェアとチェックサムとを受け取り、当該ソフトウェアよりチェックサムを生成する受信側チェックサム生成部と、この受信側チェックサム生成部で生成されたチェックサムと前記管理センタより受け取ったチェックサムとを比較する比較手段とを有する請求項10記載のソフトウェア再生管理システム。

【請求項13】 前記管理センタは、前記ソフトウェアを暗号化する暗号化部を有しており、前記送信側チェックサム生成部は前記暗号化部により暗号化される前のソフトウェアまたは暗号化された後のソフトウェアに対してチェックサムの生成を行うことを特徴とする請求項12記載のソフトウェア再生管理システム。

【請求項14】 前記請求項1のソフトウェア管理モジュールにおいて、前記請求項12の比較手段による比較結果を表示する表示手段を備えている請求項12のソフトウェア再生管理システム。

【請求項15】 前記比較手段は前記両チェックサムが等しかった場合にのみ課金情報記憶部に対して従量課金を実行する請求項12記載のソフトウェアの再生管理システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、コンピュータプログラムあるいは映像著作物等のソフトウェア、特にデジタル情報化されたソフトウェアの流通システムに適用して有効な技術に関する。

【0002】

【従来の技術】CD-ROM等の大規模記憶媒体や、B-I SDN等の大容量の高速通信技術などが発達してくると、これらの手段を用いてコンピュータプログラムは勿論、画像や音声もデジタル情報として流通されることが予想される。

【0003】すなわち、従来ビデオテープで供給されていたような映像著作物がそのままCD-ROMに格納されて販売されたり、またはCD-ROMのインタラクティブ性（双方向性）を利用したゲームとして市場に流通し始めてきている。

【0004】また、通信回線についても同様であり、前記のような映像著作物が通信を経由してユーザの手許に届けられる状況になってきている。ところで、この種のデジタル情報は他の媒体への複写が極めて容易であり、かつアナログ情報のような複写による劣化がないことから、同一情報の複製が可能であり、これらの行為により製造者の利益が害される可能性が極めて高い。すなわち、大容量の書換え可能な光磁気ディスクや磁気ディスク装置さえ所有していればわずかなDOSのコマンドの知識のみでCD-ROMの内容を複写することが簡単であった。

【0005】このように、十分なセキュリティチェックが不可能であることを理由にこの種のデジタル情報媒体のレンタル行為は製造者によって禁止されている場合が殆どである。

【0006】しかしながら、エンドユーザとしては現在のこの種のソフトウェアの価格は高額であり、本当にそのソフトウェアが自身の欲しているものと一致するか、あるいは自身の所有しているハードウェアで使用可能かの確認がとれるまでは購入を躊躇する人が多い。

【0007】この点について、機能が制限されている多数のソフトウェアをCD-ROMに格納して安価に販売し、エンドユーザはそこから希望するソフトウェアについて代金を送金することにより機能制限を解除するコードを通知されるという新しいソフトウェアの流通方式が実現され始めている。

【0008】

【発明が解決しようとする課題】しかし、前述のソフトウェアの流通方式はソフトウェアの特性を十分に反映したものとはいえなかった。

【0009】すなわち、前述の機能制限を解除する方式では、代金を一括して送金する場合が殆どであり、この代金はいきおい高額にならざるを得ず、たとえば映画の一場面を少しだけ見たいとか、1週間だけ表計算ソフト

を使用したいというような場合にその使用量に応じた料金管理は困難であった。

【0010】この点について、特公平6-19707号公報では、あらかじめ利用可能金額をICカードに登録し、有償ソフトウェアを利用する場合に前記ICカードの利用可能金額をシステムに登録して、システムが当該ソフトウェアの利用毎に残高を減算していく方式が提唱されている。

【0011】また、本出願人による特願平6-96871号公報では、CD-ROM等の記憶媒体上に書換え可能領域を設けて使用時間の情報を管理していく方式が提唱されている。

【0012】本発明は、これらの先行技術をさらに一歩進めたものであり、ソフトウェアの格納媒体を複雑にすることなく、より一層のセキュリティチェックと効率的な課金管理の可能なソフトウェアの管理方式を提案するものである。

【0013】

【課題を解決するための手段】本発明のソフトウェア管理モジュール102は、原理図である図1に示すように、プログラム、文字、図形、画像または音声等からなり暗号化された所定のソフトウェアを選択して再生するためのソフトウェア再生装置に装着され、前記ソフトウェア格納媒体とは別体で構成されたソフトウェア管理モジュールにおいて、前記暗号化ソフトウェアを入力する入力部を設け、所定の暗号化ソフトウェアの復号を許可する許可制御部を設け、前記許可制御部により許可され前記入力部で入力された暗号化ソフトウェアを復号する復号化部をさらに設けるとともに、前記復号化部で復号された復号化ソフトウェアを出力する出力部を設けた。

【0014】

【作用】前記したように、本発明では、暗号化ソフトウェアを入力する入力部104を有している。本発明では、この入力部104に入力される暗号化ソフトウェアは、同図に示すCD-ROM101のような格納媒体からのものであってもよいし、通信回線を通じて得られたデータであってもよい。またデータの種類としては、プログラムは勿論、文字、図形、画像または音声などの如何なる情報であってもよい。

【0015】入力部104の次段には前記暗号化ソフトウェアの復号を行う復号化部103が設けられている。この復号化部103は、いわゆるDES回路(Data Encryption Standard)で構成されており、CPU等で構成された許可制御部108によって制御されている。

【0016】また、復号化部103は種々の復号モードの中からソフトウェアの特性に応じて最適の復号モードが選択できるよう、モード識別部18(図3参照)を持たせてもよい。

【0017】一方、許可制御部108は、課金テーブル8(課金情報記憶部)を参照して課金残高がある場合に

のみ復号化部103での復号処理を許可するようにしてもよい。この場合、ソフトウェアの再生に応じて課金テーブル8に対して従量課金を実行する。すなわち許可制御部108は、課金テーブル8のカウント値を減算していく処理を行う。

【0018】そして、課金残高が0値となった場合には、出力部109に対して課金残高が無くなったことを通知してもよい。これによって出力部109は、出力される復号化ソフトウェアに画像データを含む場合には、画面上に課金残高が無くなったことを表示する文章をス

ーパーインポーズするようにしてもよい。
【0019】このように、本発明によれば、ソフトウェア再生装置に装着されるモジュール内に許可制御部108と、復号化部103が設けられているため、セキュリティの高いソフトウェア課金が可能となる。

【0020】さらに、課金テーブル8もこのモジュール内に収容し、この課金に関する情報（ユーザ情報）を外部に出力する場合には、暗号化部を設けて暗号化することによりセキュリティを高めることができる。この暗号化部は、具体的には前述の復号化部103と兼用すること

ができる。
【0021】さらに、復号化部103には、入力用バッファと出力用バッファとを設けてデータの入力と出力とを並列に行わせることにより復号処理を高速化できる。

【0022】

【実施例】以下に図面に基づいて本発明の実施例を説明する。図12は本発明が提案する超流通システムにおいてそれぞれの当事者（ベンダ：管理センタ、エンドユーザ：ソフトウェア再生装置、流通チャネル）に要求される技術および役割の概念を示した説明図である。

【0023】同図において示したようにベンダにおいてはチェックコード挿入や暗号化技術などのコピープロテクションに関する問題が重要となり、エンドユーザにおいてはチェックサムコードの採用によるソフトウェアの完全性保証や高速暗号化技術によるファイル転送・管理が重要となる。一方、流通チャネルにおいては、ソフトウェア販売管理機能が重視されてくる。

【0024】以上の概念を基に、本発明を具体的に説明する。図2は、本実施例に用いられるソフトウェア再生装置の構成を示す機能ブロック図である。

【0025】なお、本実施例では説明の便宜のため、入力される暗号化ソフトウェアはCD-ROMに格納されて提供されたものとするが、通信情報として得られたものであってもよい。

（ソフトウェア再生装置の構成）同図に示す破線で囲んだ部分（SD回路3）が本発明のソフトウェア管理モジュール102である。このソフトウェア管理モジュール102は、ソフトウェア再生装置内において、ボードあるいはカード形式で固定的に取付けられたものであってもよいし、ソフトウェア再生装置のカードスロット（た

例えばPCMCIA準拠のカードスロット）内に着脱自在に装着されたICカードであってもよい。

【0026】同図中、1は復調回路・制御回路であり、CD-ROMに格納されているMPEG規格の画像・音声情報を復調してデコーダ2に送出する機能を有している。デコーダ2は、エラー訂正およびビットの並び替えを実行して最大2メガバイト/秒（平均1メガバイト/秒）の画像・音声情報（暗号情報）をSD回路3に引き渡す。

【0027】ソフトウェア管理モジュール102、すなわちSD回路3では、I/O（5：入力部104）を通じて受け取った画像・音声情報（暗号情報）を復号化部103としてのDES（Data Encryption Standard）7が復号してI/O（6：出力部109）を通じてSD回路3外のデマルチプレクサ13に送出する。デマルチプレクサ13では、音声データと画像データとを分離して、MPEG処理部（MPEG-2）に出力する。MPEG処理部（MPEG-2）は、データ圧縮されたMPEG規格の画像・音声情報を伸長する機能を有しており、音声と画像が分離されて出力される際には、同期制御部（VRC）によって画像データと音声データとの同期が調整される。

【0028】そして、出力先がコンピュータ（PC）である場合にはMPEGデータはデジタル情報のまま行い、出力先がTVモニタまたはスピーカ等である場合にはD/A変換を行った後のアナログ情報として出力する。

【0029】なお、これらの情報のやりとりは許可制御部としてのソフトウェア再生装置105内の制御CPU10とSD回路3内の制御CPU4とが分担して行うが、SD回路3内の制御CPU4は制御CPU10で兼用してもよい。

【0030】本実施例のDES7は、FIP'S PUB.製の「46DATA ENCRYPTION STANDARD NIST」を使用し、MPEG処理部は、「ISO/IEC CD 13818'1~3」を使用している。

（SD回路内の機能）SD回路3では、制御CPU4が許可制御部108として機能し、CD-ROM101より読み込まれた暗号化ソフトウェアについて、DES7での復号を許可するか否かを判定する。

【0031】この判定に際して制御CPU4は、課金テーブル8を参照し、当該テーブル上に課金残高がある場合にのみDES7による復号を実行する。すなわち、課金テーブル8には所定の残高値が登録されており暗号化ソフトウェアの復号処理量または処理時間に応じて課金値が減算されるようになっている。この残高値を更新したい場合には、後述の図7に示すように、カード媒体として提供されているソフトウェア管理モジュール102を販売店等に持参し、料金を支払うことにより販売店で課金テーブル8の残高値を増加させることができる。

【0032】なお、SD回路3内に課金テーブル8を設けない場合には、当該課金値情報をFD装置12等に出し力して記録しておく必要がある。この場合に課金値情報をユーザが可読な状態でフロッピーディスク等の媒体に登録しておくセキュリティが維持できない。そこで、当該課金値等情報のユーザ情報を外部に出し力する場合には、前記制御CPU4はDES7で当該課金値情報を暗号化して暗号データとして出し力するようになっている。

【0033】すなわち、課金値情報を外部に出し力する場合にはDES7は暗号化部として機能することになる。なお、課金値情報の出し力先はフロッピーディスクに限らず、図7に示すように通信回線を経由した管理センタ31であってもよい。

【0034】一方、制御CPU4の課金テーブル8、FD装置12または管理センタ31への課金値情報の参照によって課金値が"0"であることが判明した場合の処理については後述する。(DESの詳細)図3は、DES7の概略構成を示している。DES7は同図に示すように、DES実行部15(制御CPU4で実現される)を有しており、入力データ(IN)を鍵情報16により復号して出し力データ(OUT)として出し力する機能を有している。

【0035】本実施例において、DES実行部15はモード識別部18を有しており、このモード識別部18は複数のDESモードの中からそのデータ形式等により最適なモードを選択してDES実行部15に与える機能を有している。

(DESモードの説明)次に前記DESモードのうち、代表的なロジックを説明する。

【0036】図4(a)は、ECB基本モードであり、DES実行部15において、64ビットの鍵情報16により64ビットの入力データ列を64ビットの出し力データ列として暗号化(または復号化)するモードである。

【0037】図4(b)は、CBCモードを示しており、DES実行部15において64ビットの入力データ列を64ビットの鍵情報16で暗号化(または復号化)した後、再度これをDES実行部15に帰還入力させる。このようにデータを全て入力し終るまでフィードバックを行い最終結果を出し力する方式であり、ファイル等のデータ処理に適している。

【0038】図4(c)は、OFBモードを示しており、エラーの生じやすい通信データや、一つの誤りが他に与える影響の大きい音声データ等に適している。図4(d)は、CFBモードであり、自己同期形のデータに適している。

【0039】前述のモード識別部18はモードテーブル20に格納されたこれらのモードのうちデータ形式等を解析して最適なものを読み出してDES実行部15に送出する。DES実行部15ではこのようにして選択されたモードに基づいて暗号化・復号化処理を行う。

(DES実行部の高速演算処理化)図5は、DES実行部15のハードウェア構成を示すブロック図である。

【0040】同図において、入力側には入力用バッファとして、8ビット構成のレジスタが8個接続されて64ビットのシフトレジスタ(入力レジスタ21:REG1)が配置されており、次段にはセクタselが配置されている。当該セクタselは、後述のDES処理メイン回路25からの出し力か、前記シフトレジスタ21からの出し力かを選択的に入力できるようになっている。

【0041】セクタselの次段には8ビット構成のレジスタ23(REG2)が配置されさらにその次段にはDES処理メイン回路25が配置されている。このDES処理メイン回路25がDES実行部15として機能する。すなわち、DES処理メイン回路25には、図4で説明した各種のDESモードがROM(Read Only Memory)として登録されており、制御CPU4からの指示により最適なDESモードのロジックを選択して復号処理を行うようになっている。

【0042】前記DES処理メイン回路25の出し力は前記セクタselと出し力用バッファとしての出し力レジスタ24(REG3)に分岐されている。そして出し力レジスタ24(REG3)の出し力が暗号化または復号化されたデータとして用いられる。

【0043】この処理のシーケンスを示したものが図6である。図6において、入力レジスタ21の出し力は、次サイクルの最初のクロックでレジスタ23からの出し力としてDES処理される。そして次のクロックで出し力レジスタ24より出し力される。この出し力レジスタ24からの出し力時間に入力側では入力レジスタ21より次サイクルの暗号化データの取り込みが行われている。

【0044】このように、本実施例では入力用バッファとしての入力レジスタ21と、出し力用バッファとしての出し力レジスタ24とを設けたことにより、暗号化データの入力と復号化データの出し力とをそれぞれ独立して連続的に行うことができるようになった。そのため、従来のDESのようにサイクリックに入力と出し力とを行う場合に較べて高速な復号化・暗号化処理が可能となった。

(本発明を用いたソフトウェア流通形態の全体像)図7は、本発明によって実現されるソフトウェア流通の全体像を示している。

【0045】本実施例においてソフトウェアは、出荷センタ(ここでは便宜的に管理センタが出荷センタを兼ねているものとする)より流通経路に出荷されるが、このときの形態は、暗号化したソフトウェアをCD-ROMに格納した状態であってもよいし、通信路上に出荷してもよいし、あるいは光磁気ディスク等の媒体で出荷してもよい。

【0046】エンドユーザは販売店27等に赴き(通信販売でもよい)、ソフトウェアが格納されたソフトウェア格納媒体101としてのCD-ROMを購入してく

る。またこれと同時に、当該ソフトウェアを自身のソフトウェア再生装置105で再生可能ようにドライバソフトウェア等の運用アプリケーションディスク26およびソフトウェア管理モジュール102であるSDカードを購入してくる。ここで、運用アプリケーションディスク26はたとえばフロッピーディスクの形態であり、これを外部ユーザ情報格納媒体106として用いてもよい。また、CD-ROMは複数のソフトウェアが格納されているものの、このCD-ROMを売り切る販売方式ではないため、CD-ROM自体の販売価格は非常に安価に設定されている。また販売店27はレンタル店であってもよい。

【0047】すなわち、本発明ではCD-ROMに格納されたソフトウェアは全て暗号化されており、これを復号して再生する場合にはセキュリティの高く保持されたソフトウェア管理モジュール102としてのSDカードを用いることが必須である。そして後述のようにソフトウェアの使用量に応じた料金徴収システムが完備されている。したがって、CD-ROM自体に格納されている暗号化データを他の媒体に複写したとしてもそれだけでは意味がなく、CD-ROMをレンタル方式としても使用量に対応した料金徴収システムが完備されていればソフトウェア提供者の利益を低下させてしまうことはない。

【0048】エンドユーザは、自己のソフトウェア再生装置105で当該CD-ROM(101)に格納されたソフトウェアの再生を望む場合には、まずSDカード(102)をカードドライブ装置28に挿入し、CD-ROM(101)と運用アプリケーションディスク26ソフトウェア再生装置105にそれぞれ装填する。

【0049】そして、ソフトウェア再生装置105にインストールされた通信アプリケーション(このアプリケーションは運用アプリケーションとして提供されるものでもよい)を起動して、ソフトウェア再生装置105に内蔵されたモデム(変調装置)より家庭用電話機30を通じて管理センタ31に対して使用したいソフトウェアの使用要求を発信する。これに対して管理センタ31は、当該ユーザに対して許諾コマンド(鍵情報)を暗号化してソフトウェア再生装置105に対して送出する。

【0050】前記許諾コマンドを受け取ったソフトウェア再生装置105は、CD-ROM101を読み取り、必要なソフトウェアをSDカードの復号部103を通じて順次復号化してソフトウェア再生装置105のプログラム格納エリア(メモリ)に転送する。

【0051】これとともに、制御CPU4は当該ソフトウェアの復号データ量、または復号時間をカウントし、課金テーブル8より課金残高値を減算する。そしてこの課金残高値が"0"になるまでは暗号化ソフトウェアの復号処理を継続する。

【0052】ここで、課金テーブルの課金残高値が

0"となった場合には、復号化ソフトウェアの出力を停止する。この出力停止を具体化するハードウェア構成を図8に示している。

【0053】すなわち、同図では、課金テーブル8を監視していた制御CPU3は、課金テーブル上の課金残高値が"0"となったことを検出したとき、この情報をソフトウェア再生装置105内の制御CPU10に通知する。この通知に基づいて制御CPU10はレジスタ81の保持値を変化させて、TVモニタへの出力およびコンピュータ(PC)への出力段にある論理積回路(AND83)とアナログスイッチ(SW82)を閉じる。これによって出力装置へはアナログ変換された音声情報しか出力されない。

【0054】なお、これとともに画像出力として課金残高が"0"となった旨の表示あるいは広告等をスーパーインポーズしてもよい。以上の説明は課金残高をSD回路3内の課金テーブル8が管理している場合の例であるが、この課金値残高情報は管理センタ31が管理していてもよい。この場合、課金値残高情報がソフトウェア再生装置105の外部に出力されることになるので、セキュリティを高めるために前述の制御CPU3は、DES7を用いて課金値残高情報を暗号化して、暗号化データとして電話回線を通じて管理センタ31に通知する。

【0055】管理センタ31ではソフトウェア再生装置105から受領した課金値残高情報にしたがって、金融機関32のエンドユーザの口座よりエンドユーザが使用した使用量に応じた料金を引き落として当該ソフトウェア提供者の口座に送金する処理を行う。

【0056】このように、本発明ではCD-ROMに格納されたソフトウェアばかりでなく、そのソフトウェアの運用によって生じたユーザ情報も暗号化して外部に出力するため、ユーザ情報の改ざんによるソフトウェアの不正使用も防止することができる。

(出荷されたソフトウェアの完全性保証について)ところで、ソフトウェアの流通経路においてソフトウェアにウィルス等が混入され、エンドユーザはウィルスが混入されたソフトウェアを再生することにより、ハードウェアや自己の蓄積したソフトウェアを破壊されたり、さらにはウィルのために正常に動作しないソフトウェアに対しても課金されるおそれが生じてくる。

【0057】このような流通経路におけるウィルス混入をソフトウェア再生装置105において確実に検出できるようにした構成が図9である。すなわち、管理センタ31にはチェックサム生成部111aが設けられている。このチェックサム生成部111aは出荷すべきソフトウェアからチェックサム(CS)、すなわちデータの完全性をチェックするコードを生成する機能を有しており、本実施例ではハッシュ関数による関数コードがチェックサム(CS)として出力されるようになっている。

【0058】このチェックサム生成部111aのロジッ

クを示したものが図11である。すなわちここでDES暗号による操作を行う場合、基本的にはCBCモード（図4（b）で説明したもの）を構成しており、プログラムあるいはデータを1ブロック単位に区切り、CBCモード（ブロック帰還）で一旦出力したデータをそのまま帰還入力し、次の入力ブロックとで排他論理和制御（EOR）を行う。この結果を再びDES暗号化処理して前記と同様に出力を入力側に帰還させる。そして最終ブロックが入力された場合、変換された暗号化出力をチェックサム（CS）とする。

【0059】図10は、ソースプログラムをコンパイラによりオブジェクト化した後、圧縮処理を施しこの圧縮平文オブジェクトプログラムをハッシュ関数hに入力して（チェックサム生成部111aで処理して）、チェックサム（CS）を得、これを前記圧縮平文オブジェクトプログラムに結合する様子を示している。

【0060】このような暗号化プログラムが流通経路を流通した段階でコンピュータウィルスが混入された場合、ソフトウェア再生装置105における下記の機構を用いることによりウィルス混入の確認が容易となる。

【0061】すなわち、ソフトウェア再生装置105には、前記チェックサム生成部111aと同様のチェックサム生成部111bを有しており、ソフトウェアより前記と同様の方法でチェックサム（CS'）を生成する。そして、比較部112において前記ソフトウェアに添付されてきたチェックサム（CS）と前記チェックサム生成部111bで新たに生成されたチェックサム（CS'）とを比較する。

【0062】このとき、流通経路上でソフトウェアにウィルスが混入し、ソフトウェアの改変が行われると、チェックサム生成部111bで生成されるチェックサム（CS'）は必然的に元のチェックサム（CS）とは異なる。

【0063】このように比較部112が比較結果に異常を検出したときには表示部113において異常を示す赤色表示を行う。この表示はたとえばカード形状で構成されたソフトウェア管理モジュールの一端にスイッチ（SW）によりその表示状態を変更可能な表示ランプを設けることにより容易に実現できる。また、チェックサム生成部111bが処理を行っている間は処理中である黄色表示を行い、比較結果が等しく正常終了した場合には青色表示を行うようにした。

【0064】そして、比較部112での比較処理が正常終了した場合にのみ課金テーブル8から従量課金を実行する。具体的には許可制御部108（図9では図示省略）が課金テーブル8のカウント値を減算していく処理を行う。

【0065】図9および図10で説明したチェックサム生成と、暗号化との関係についてさらに詳しい具体例で示したものが図13～図22である。これらの図ではソ

フトウェアはCD-ROMに格納されて情報提供者（管理センタ）からエンドユーザ（ソフトウェア再生装置）に供給される場合を想定している。

【0066】図13は、平文のソフトウェアから鍵情報（K1）を用いてチェックサム（CS）を生成し、これをCD-ROMの所定領域に格納している。そして、前記平文ソフトウェアは鍵情報（K2）を用いて暗号化してCD-ROM上の前記チェックサム（CS）の格納された領域以外の領域に格納し、これをエンドユーザに提供する。エンドユーザは、ヘッダ解析を行いながら暗号化ソフトウェアを鍵情報（K2）で復号しこれを一旦メモリまたはそれ以外の記憶手段に蓄える。そして、復号化された平文ソフトウェアから鍵情報（K1）を用いてチェックサムを生成し、これをCD-ROMから読み出されたチェックサムと比較する。そして、比較結果が一致した場合にのみ課金処理を実行する。

【0067】図14は、図13の例において、情報提供者（管理センタ）において暗号化処理を行わない場合である。図15は、暗号化された情報（ソフトウェア）からチェックサムを生成する点の特徴である。すなわち、平文ソフトウェアを鍵情報（K2）でまず暗号化してこれをCD-ROMに格納する。そして暗号化ソフトウェアに対してチェックサムを生成しこれを所定の領域に格納しエンドユーザに供給する。

【0068】エンドユーザ側ではヘッダ解析を行いながら暗号化ソフトウェアから直接チェックサムを生成し、このチェックサムをCD-ROMに格納されていたチェックサムと比較する。

【0069】図16は、情報提供者（管理センタ）側の処理は図13と同様であるが、エンドユーザ側（ソフトウェア再生装置側）の課金処理が異なっている。すなわち、ヘッダ解析の結果課金処理を開始するが、チェックサムの比較結果が一致しなかった場合には課金処理を無効（旧状態復帰書換）にするようになっている。

【0070】図17は、情報提供者（管理センタ）側の処理は図14と同様であるが、エンドユーザ側（ソフトウェア再生装置側）の課金処理が異なっている。すなわち、ヘッダ解析の結果課金処理を開始するが、チェックサムの比較結果が一致しなかった場合には課金処理を無効（旧状態復帰書換）にするようになっている。

【0071】図18は、情報提供者（管理センタ）側の処理は図15と同様であるが、エンドユーザ側（ソフトウェア再生装置側）の課金処理が異なっている。すなわち、比較結果に基づいて課金処理を実行しこの課金処理によって復号を開始するようになっている。

【0072】図19は、情報提供者（管理センタ）側の処理は図16と同様であるが、エンドユーザ側（ソフトウェア再生装置側）の課金処理が異なっている。すなわち、ヘッダ解析の結果課金処理を開始するが、チェックサムの比較結果が一致しなかった場合には課金処理を無

効(旧状態復帰書換)にするようになっている。

【0073】図20は、情報提供者(管理センタ)側の処理は図15と同様であるが、エンドユーザ側(ソフトウェア再生装置側)の課金処理が異なっている。すなわち、ヘッダ解析の結果課金処理を開始するが、チェックサムの比較結果が一致しなかった場合には課金処理を無効(旧状態復帰書換)にするようになっている。

【0074】図21は、平文ソフトウェアを鍵情報(K)で暗号化するとともに特定の領域nに暗号化データの一部Nに対応した情報を登録しておき、エンドユーザ側(ソフトウェア再生装置)で前記Nを復号し、これをnと比較するものである。そして比較の結果が一致すれば課金処理を行うようになっている。

【0075】図22は、情報提供者(管理センタ)側の処理は図21と同様であるが、ヘッダ解析とともに課金処理を開始し、比較結果が一致しなかった場合には課金処理を無効(旧状態復帰書換)にするようになっている。

【0076】以上説明したように、図9～図22に示した例では、データの完全性保証の確認が容易であるため、ウィルスが混入されたソフトウェアを再生することにより生じるハードウェアあるいはデータの破壊、不合理な課金を未然に防止できる。

(管理センタによるソフトウェアの貸出時刻管理)次に管理センタ31によりソフトウェアの利用時刻管理が行われる場合について説明する。

【0077】前記管理センタ31はソフトウェア再生装置105に対して許諾コマンドを発行するとともに、コンテンツに対応する利用開始時刻(タイムスタンプ)を暗号化して通信回線を通じて(モデム経由でも可)ソフトウェア再生装置105に送出する。

【0078】ソフトウェア再生装置105では、このタイムスタンプを受け取ると自身のSD回路3でこのタイムスタンプを復号し、課金テーブル8に書き込む。このときコンテンツ毎に課金テーブル8が設定されているときには該当欄にタイムスタンプを書き込むようにする。

このように、タイムスタンプを管理することによりエンドユーザのソフトウェアの利用期限を管理することができる。

【0079】なお、暗号化タイムスタンプの配送は、管理センタ31のオペレータがエンドユーザに対して口頭で伝え、エンドユーザがこれをキーボード等を通じて自身のソフトウェア再生装置105に入力するようにしてもよい。このようにしてもタイムスタンプは暗号化されているため、セキュリティは保持できる。

【0080】なお、以上説明した実施例において、ソフトウェア再生装置105へのソフトウェアの提供は、CD-ROMのような有形媒体のみに限らず、高速化された通信システムを経由してホストコンピュータより通信データとして得られたソフトウェアであってもよいこと

は勿論である。

【0081】

【発明の効果】本発明によれば、ソフトウェアの格納媒体を複雑にすることなく、より一層のセキュリティチェックと効率的な課金管理の可能なソフトウェアの管理を行うことができる。

【図面の簡単な説明】

【図1】 本発明の原理図

【図2】 本実施例のソフトウェア再生装置を示す機能ブロック図

【図3】 本実施例のDESの内部機能を示すブロック図

【図4】 DESの各モードを示す説明図

【図5】 DES実行部のハードウェア構成を示すブロック図

【図6】 DES実行部の処理シーケンスを示す説明図

【図7】 本発明のソフトウェア流通システムの全体概念を示す説明図

【図8】 実施例において、課金テーブルの残高によって出力を停止するためのハードウェア構成図

【図9】 実施例において再生されるソフトウェアの完全性保証を確認するための機構を示すブロック図

【図10】 実施例において再生されるソフトウェアの完全性保証を確認するためのデータの構成を示すブロック図

【図11】 実施例におけるチェックサム生成部の機能を示すブロック図

【図12】 本発明においてそれぞれの当事者に要求される技術、役割の概念を示した説明図

【図13】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図14】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図15】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図16】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図17】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図18】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図19】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図20】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図21】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図22】 管理センタとソフトウェア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【符号の説明】

15

1・・・復調回路・制御回路、
 2・・・デコーダ、
 3・・・SD回路、
 4・・・制御CPU、
 5・・・インターフェース(I/O)、
 6・・・インターフェース(I/O)、
 7・・・DES
 8・・・課金テーブル、
 10・・・制御CPU、
 11・・・インターフェース、
 12・・・フロッピーディスク装置、
 13・・・デマルチプレクサ、
 15・・・DES実行部、
 16・・・鍵情報、
 18・・・モード識別部、
 20・・・モードテーブル、
 21・・・入力レジスタ、
 23・・・レジスタ、
 24・・・出力レジスタ、
 25・・・DES処理メイン回路、

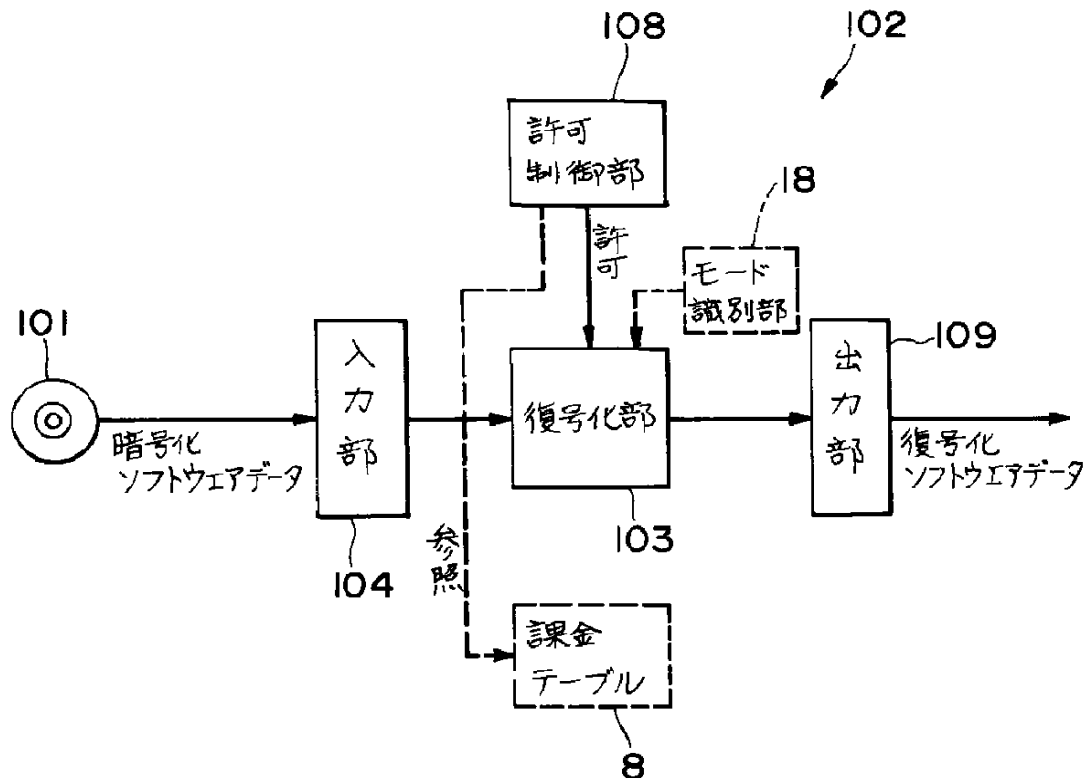
16

26・・・運用アプリケーションディスク、
 27・・・販売店、
 28・・・カードドライブ装置、
 30・・・家庭用電話機、
 31・・・管理センタ、
 32・・・金融機関、
 101・・・ソフトウェア格納媒体、
 102・・・ソフトウェア管理モジュール、
 103・・・復号化部、
 105・・・ソフトウェア再生装置、
 106・・・外部ユーザ情報格納媒体、
 107・・・メモリ、
 108・・・許可制御部、
 111a, 111b・・・チェックサム生成部
 112・・・比較部
 113・・・表示部
 DB・・・データベース、
 NT・・・ネットワーク、
 sel・・・セレクト、

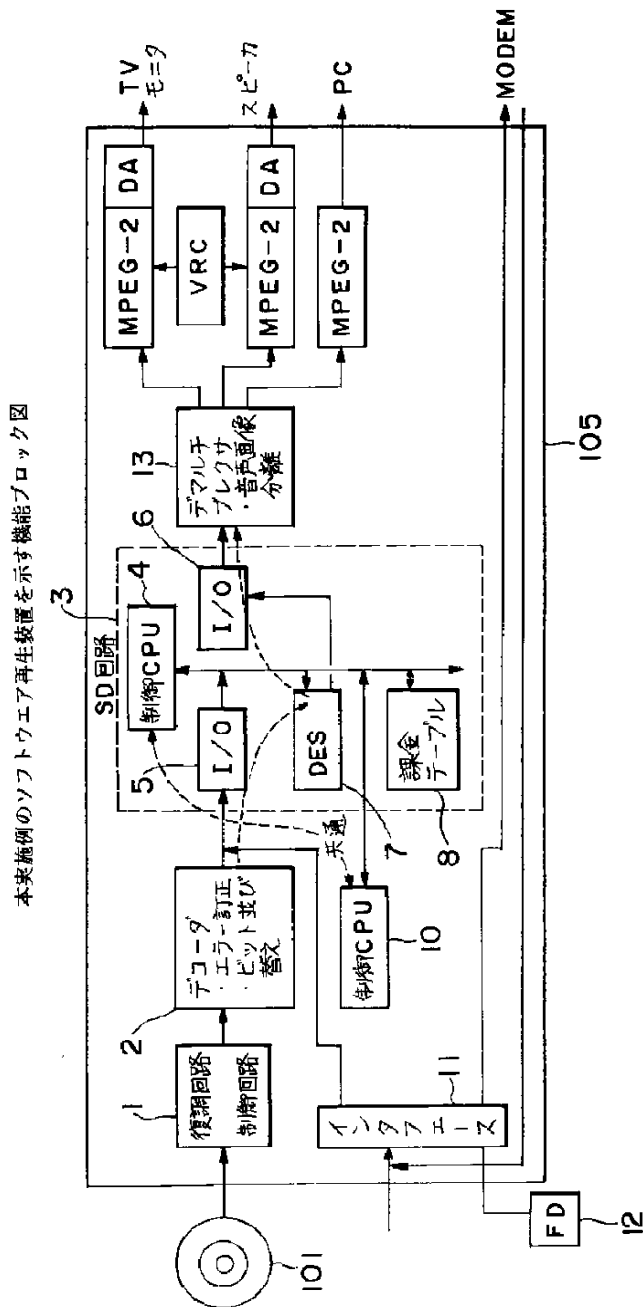
20

【図1】

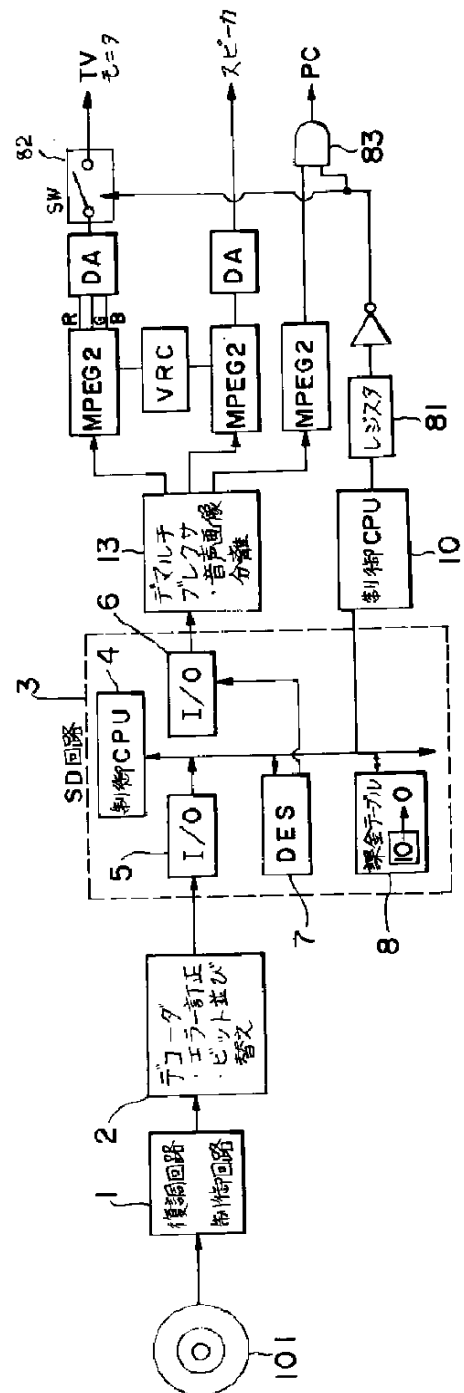
本発明の原理図



【図 2】



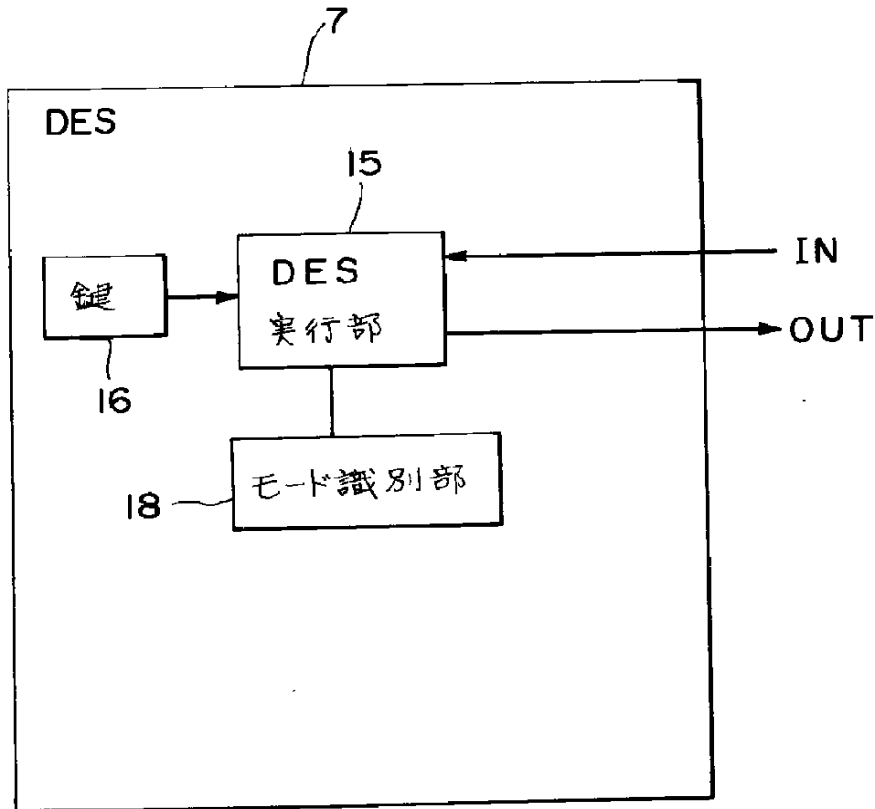
【図 8】



実施例において、課金テーブルの残高によって出力を停止するためのハードウェア構成図

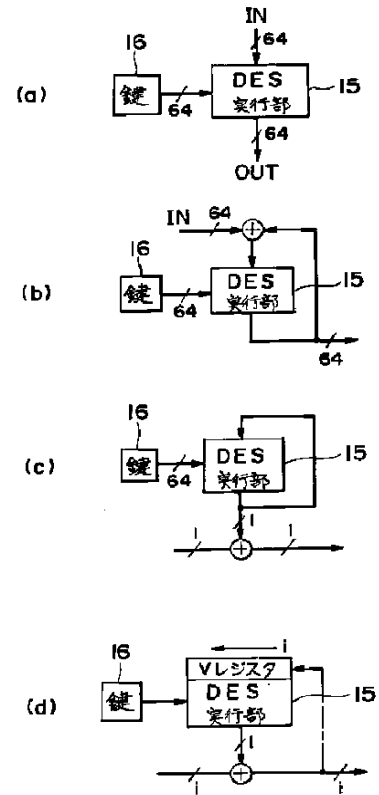
【図3】

本実施例のDESの内部機能を示すブロック図



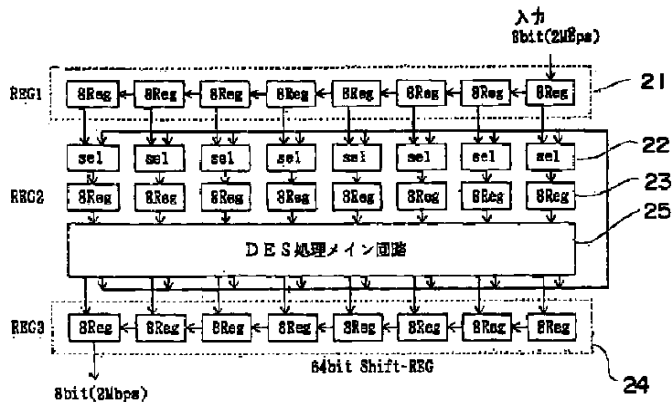
【図4】

DESの各モードを示す説明図



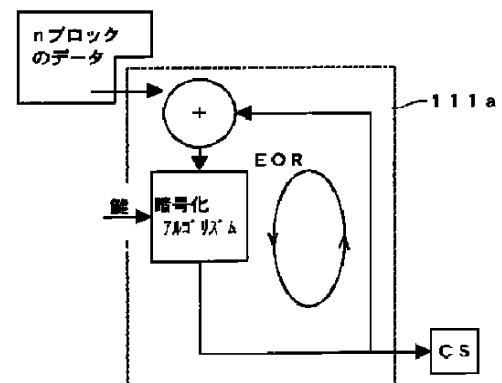
【図5】

DES 実行部のハードウェア構成を示すブロック図

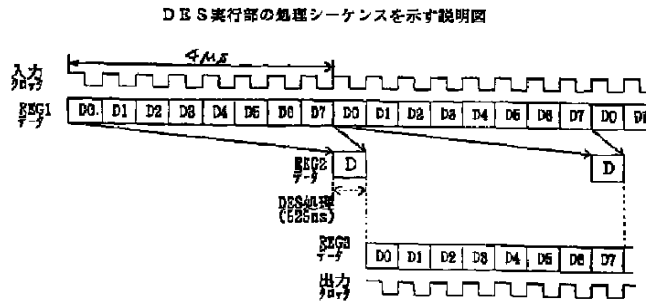


【図11】

実施例におけるチェックサムコード生成部の機能を示すブロック図

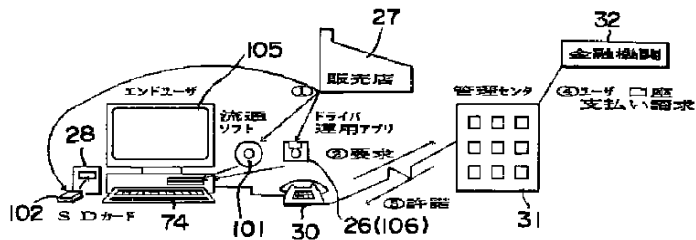


【図6】

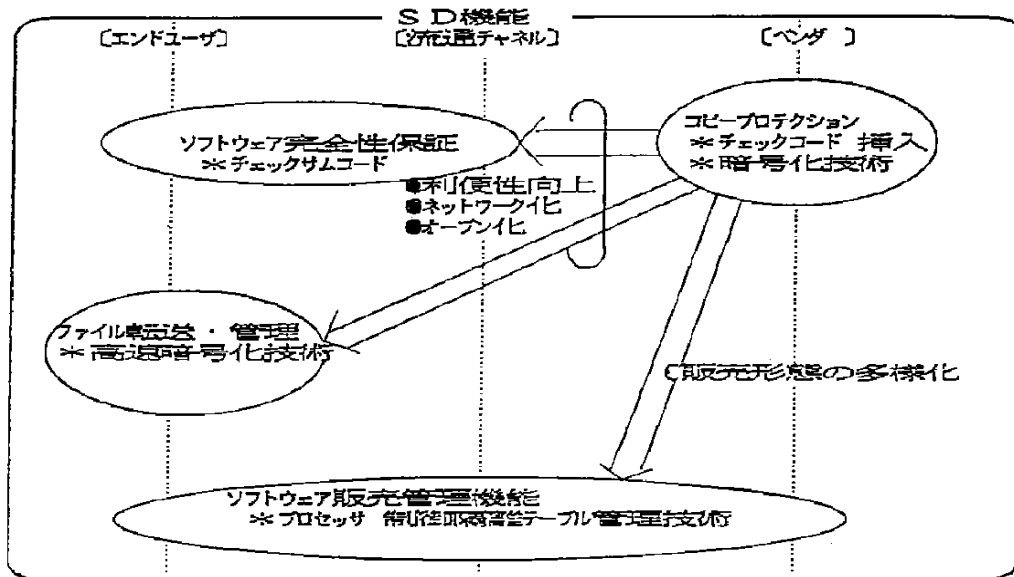


【図7】

本発明のソフトウェア流通システムの全体概念を示す説明図

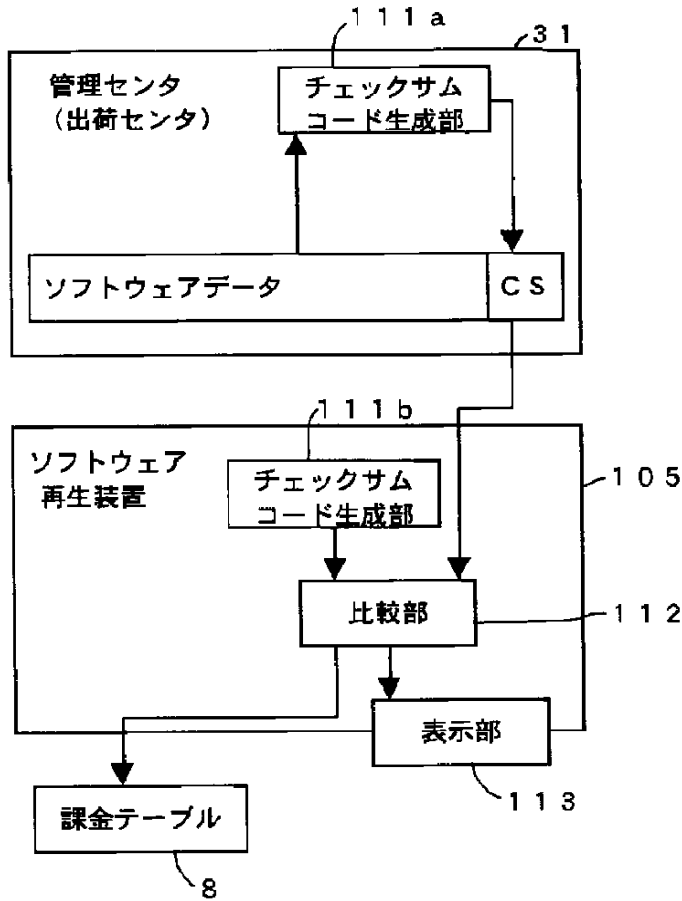


【図12】

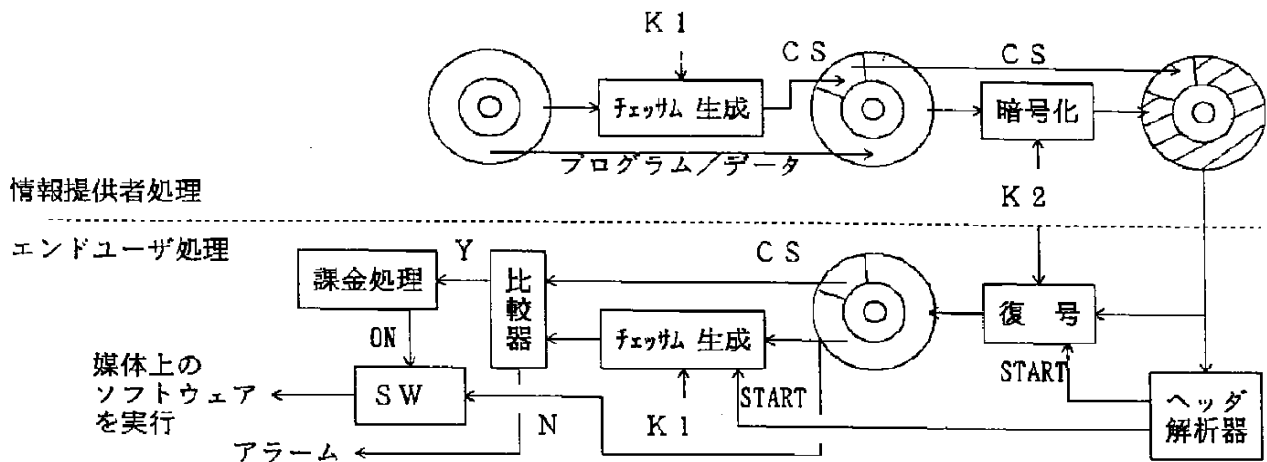


【図9】

実施例において再生されるソフトウェアデータの完全性保証を確認するための機構を示すブロック図

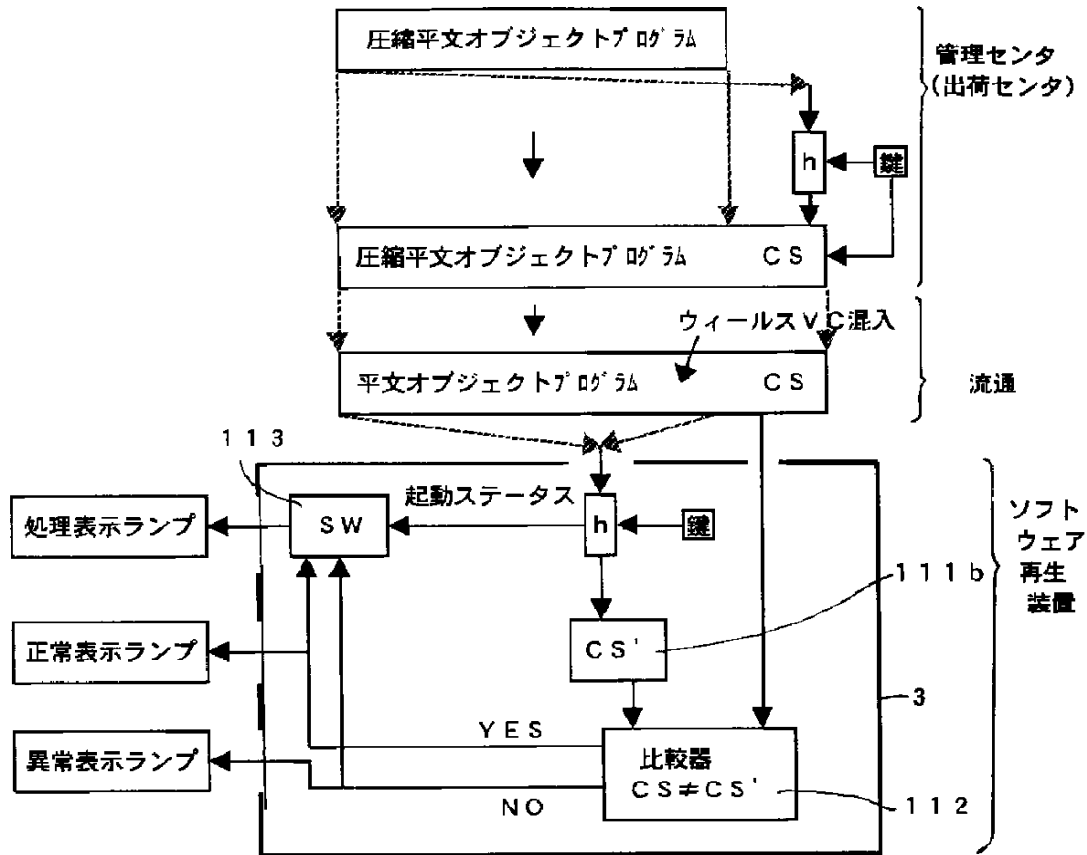


【図13】

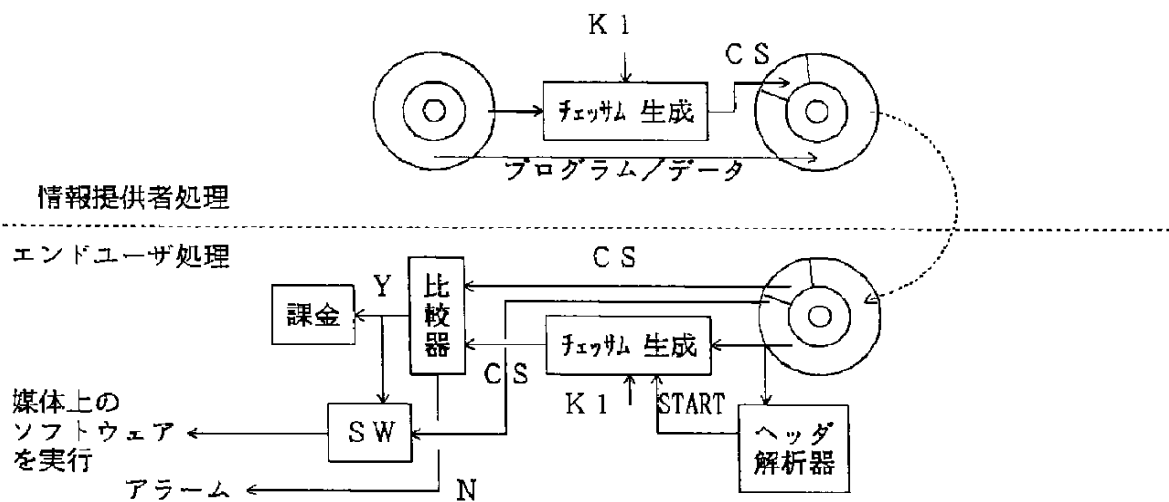


【図10】

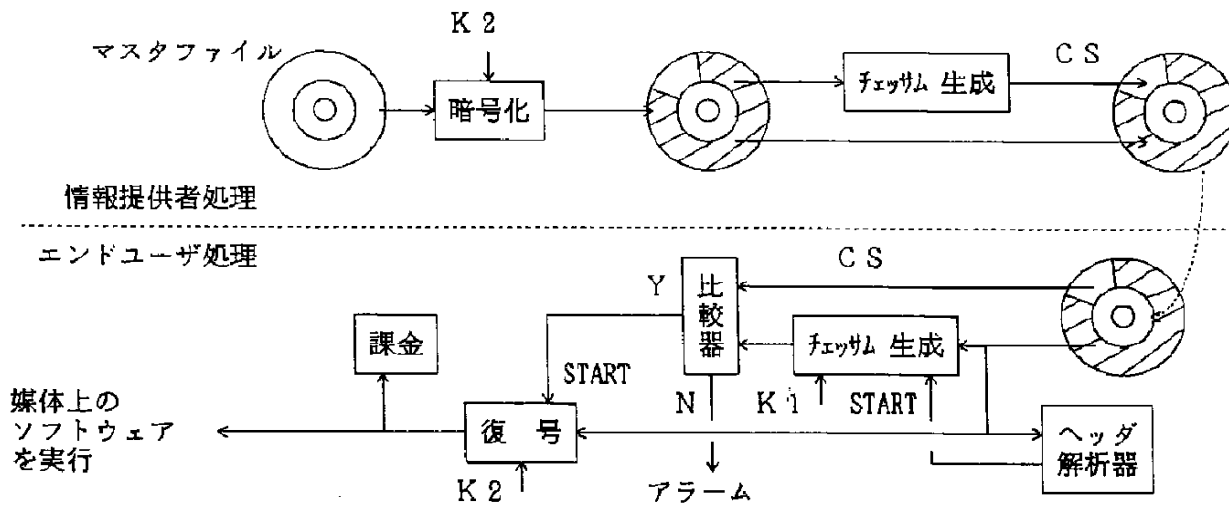
実施例において再生されるソフトウェアデータの完全性保証を確認するためのデータの構成を示すブロック図



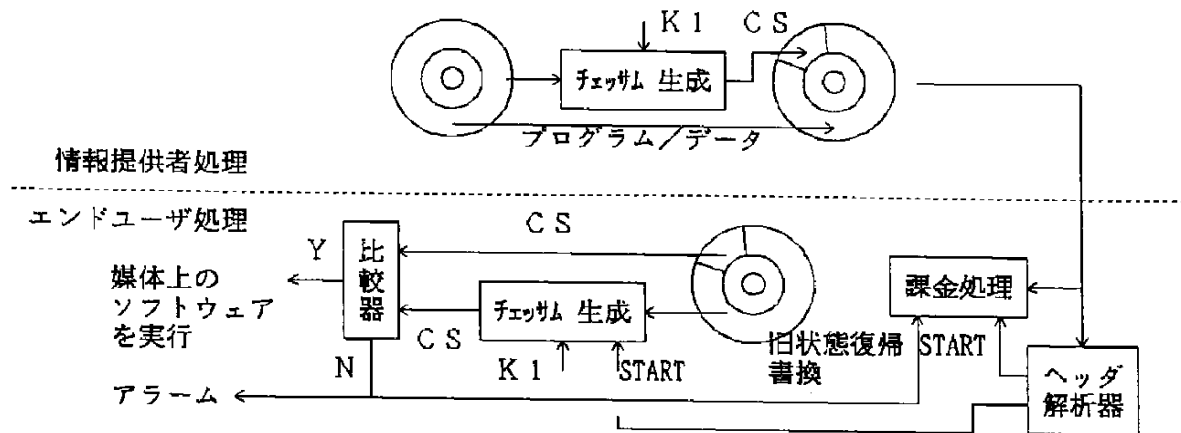
【図14】



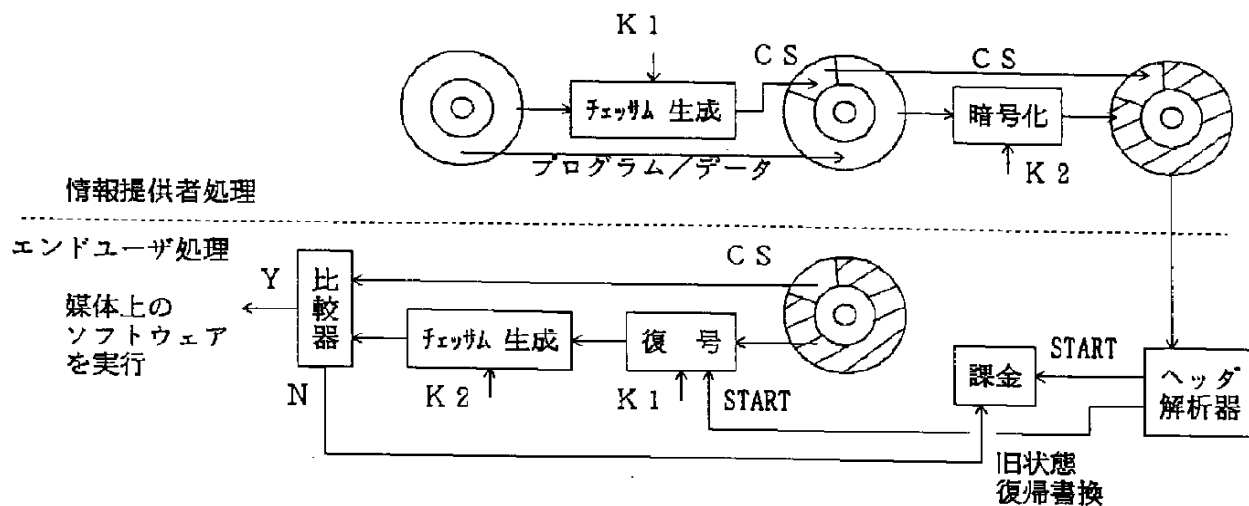
【図15】



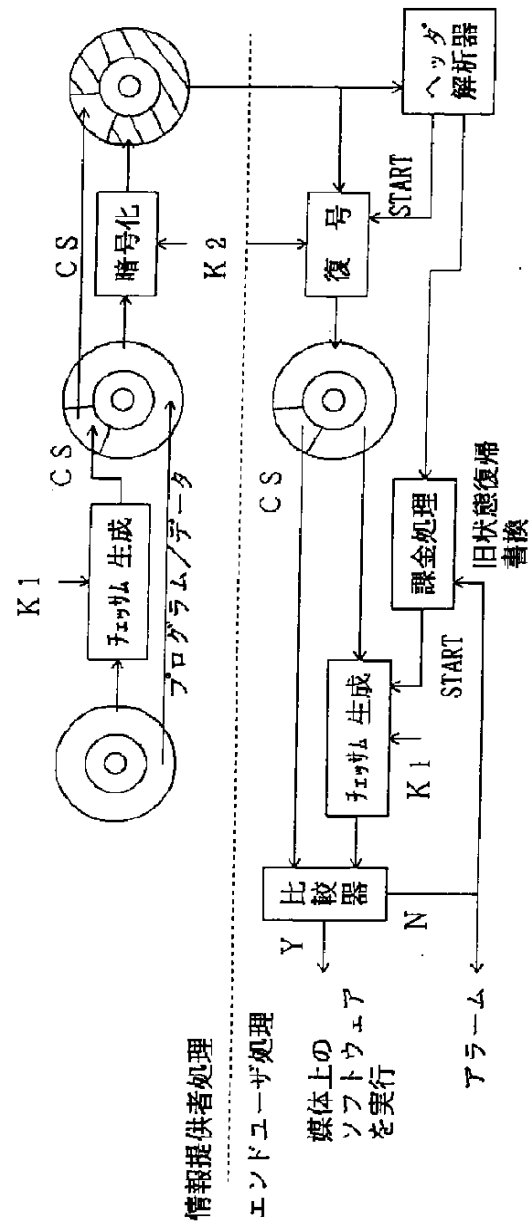
【図17】



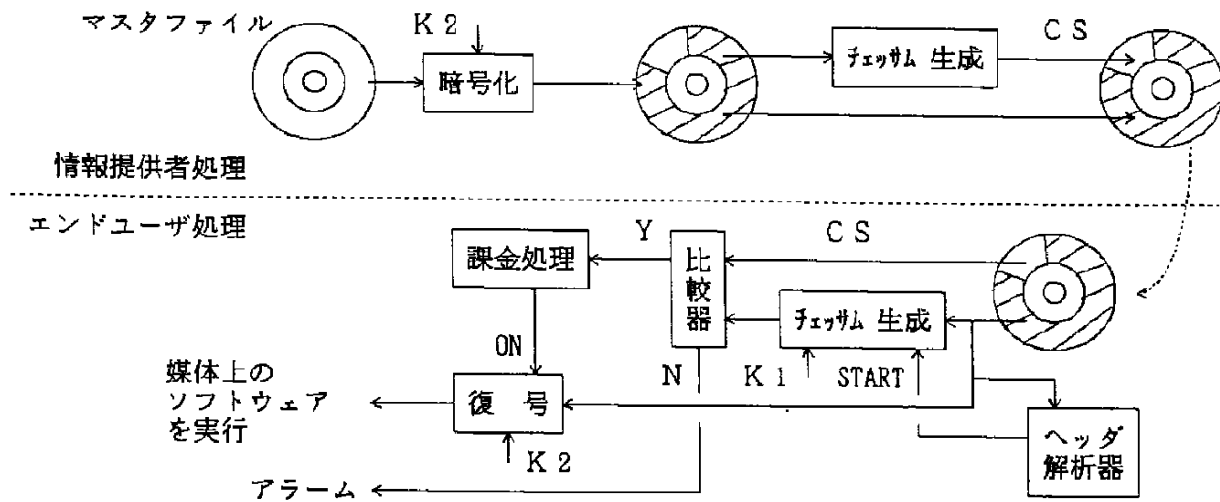
【図19】



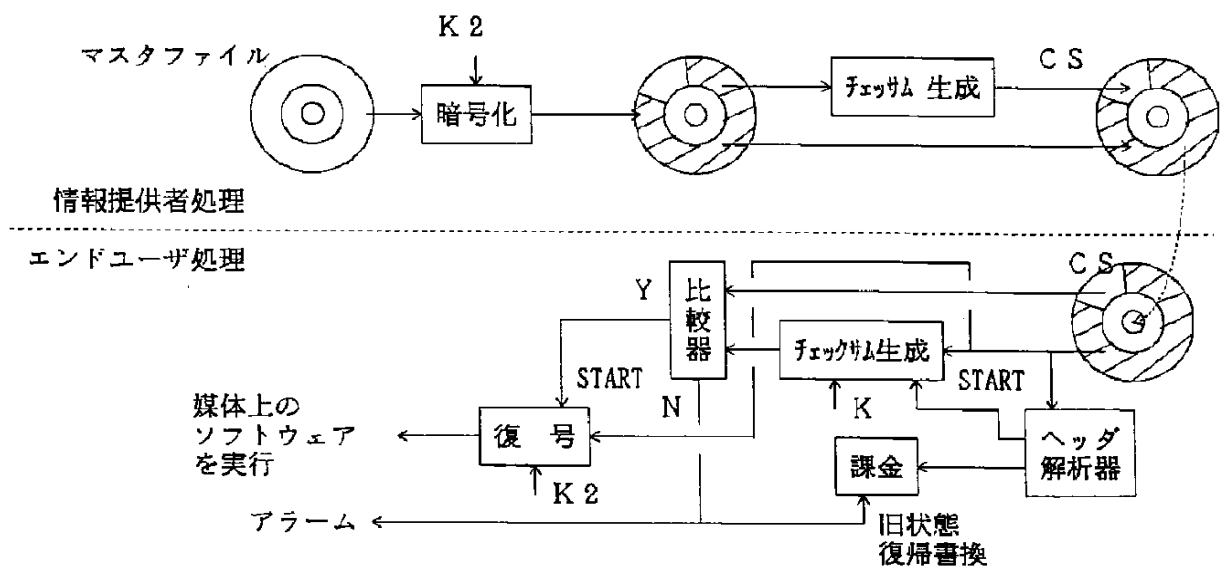
【図16】



【図18】



【図20】



SOFTWARE MANAGEMENT MODULE AND SOFTWARE REPRODUCTION MANAGEMENT DEVICE/SYSTEM

Publication number: JP8106382 (A)

Publication date: 1996-04-23

Inventor(s): AKIYAMA RYOTA; YOSHIOKA MAKOTO

Applicant(s): FUJITSU LTD

Classification:

- **international:** **G06F21/22; G06F1/00; G06F21/00; G09C1/00; G06F21/22; G06F1/00; G06F21/00; G09C1/00; (IPC1-7): G06F9/06; G09C1/00; G11B19/02**

- **European:** G06F21/00N7P5H; G06F21/00N7D

Application number: JP19940225228 19940920

Priority number(s): JP19940225228 19940920; JP19940219372 19940810

Also published as:

JP3395863 (B2)

EP0702286 (A2)

EP0702286 (A3)

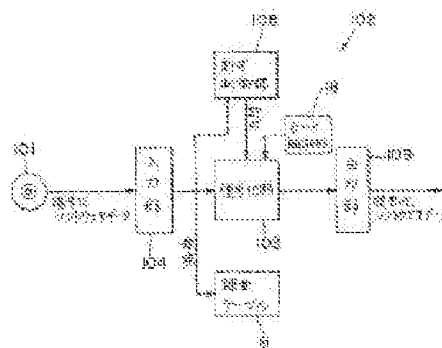
EP0702286 (B1)

US5737415 (A)

Abstract of JP 8106382 (A)

PURPOSE: To improve the security check efficiency and to attain the effective charging management without complicating the structure of a software storing medium by decoding the inputted ciphered software and then outputting this decoded software.

CONSTITUTION: A decoding part 103 includes a mode identification part 18 which consists of a DES and is controlled by a permission control part 108 to select the optimum one of various decoding modes in response to the software characteristic. The part 108 refers to a charging table 8 and permits the part 103 to perform a decoding processing job only when the charging balance is confirmed. Then the part 108 carries out the imposing a charge at a rate per unit of quantity to the table 8 in response to the reproduction of software and also informs an output part 109 of a fact that the charging balance is zero.; Thus both parts 108 and 103 are included in a module that is loaded into a software reproduction device so that the software charging is attained with high security.



.....
Data supplied from the **esp@cenet** database — Worldwide